UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,794	01/17/2001	Vinay Deo	M61.12-0685	8460

7590 07/12/2004

John A. Wiberg
Westman, Champlin & Kelly
Suite 1600
International Center 900 Second Avenue South
Minneapolis, MN 55402-3319

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	5

DATE MAILED: 07/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/764,794	DEO ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *37-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *37-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 4/29/04 was received and considered.

2. Claims 37-44 are pending.

Response to Arguments

3. Applicant's arguments, with respect to claim 37 have been fully considered and are persuasive. The rejection of claim 37 has been withdrawn.

4. Applicant's arguments, see page 6, ¶1-2, filed 4/29/04, with respect to the rejection(s)of claim(s) 37-44 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of U.S. Patent 6,496,928.

5. As per applicant's amendments, the objections to the claims have been withdrawn.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 37, 38 & 44 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 & 24 of U.S. Patent No. 6,496,928 in view of Applied Cryptography, Second Edition by Bruce Schneier, in further view of "Cryptography Terminology" by EFA. The '928 patent claims in claim 1 a substantially equivalent invention as claims 37 & 38 of the instant application and claims in claim 24 a substantially equivalent intention as claim 44 of the instant application, but the '928 patent does not teach a first data string being further used to generate the first key, a second key generated from a second data string, base key and message specific data, generating a signature with a hash using the first key and encrypting the message and signature with the second key. However, Schneier teaches that adding signatures to documents allows the receiver to be convinced of the document's authenticity (page 39, ¶1-4). Signatures can be performed using one-way hash functions to save time (page 38, §Signing Documents ... One-Way Hash Functions). Schneier further teaches that message authentication codes are key-dependent one-way hash functions used to authenticate files/messages between users with the key (page 455, §18.14). Further, EFA teaches that it is recommended that a different key be used for signature and encryption in a system where a signature is appended to a message (page 1, §Digital Signature). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to create a second key, obtain a signature by hashing the message with the first key and append it to the document and encrypt the message and appended signature using the second key. One of ordinary skill in the art would have been motivated to perform such a modification, as is recommended to do so, as taught by EFA (page 1, §Digital Signature), and to verify the authenticity of the document, as taught by Schneier (pages 38-39). As modified, claims 1 & 24

of the '928 reference, respectively, '928 reference lack a first and second data string used in key generation. However, Schneier teaches that adding a salt to a password/key is beneficial to make a dictionary attack on the password/key less successful (page 52, §Dictionary Attacks and Salt). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a first and second data string in the generation of the first and second keys. One of ordinary skill in the art would have been motivated to perform such a modification to increase the keyspace and hence make dictionary attacks less successful, as taught by Schneier (pages 52-53).

8. Claims 39-40 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 6,496,928 in view of Schneier and EFA, as modified above, in further view of U.S. Patent 6,049,018 to Hardy et al. (Hardy). Claim 1 of the '928 reference lacks the first and second encryption key components hashing the base key, data strings and message-specific data to obtain a bias value, which is used to obtain the keys via the key generator. However, Hardy teaches a pseudo-random key can be generated by combining a document digest/message-specific data and at least one other secret value (such as the base key) using a hash, and inputting the result to a predefined pseudo-random key generator (col. 7 line 60 – col. 8 line 34). Hardy's system has the benefit of a reliably distinct key for each document/message signed (col. 7 lines 48-57). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to hash the message-specific data, base key and data strings to obtain bias values to input to a key generator component configured to receive the bias value and generate the encryption keys based

on the biased values. One of ordinary skill in the art would have been motivated to perform such a modification to obtain a reliably distinct key for each document/message signed, as taught by Hardy (col. 7 lines 48-57).

9. Claims 41-43 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 24 of U.S. Patent No. 6,496,928 in view of Schneier and EFA, as modified above, in further view of U.S. Patent 5,701,316 to Alferness et al. (Alferness). Claim 24 of the '928 reference lacks creating a checksum over the message and appending it to the message so that a checksum can be created and compared to determine whether the message is valid. However, Alferness teaches that with increasing traffic across networks, there is a need to perform checksum calculations as a means to detect transmission errors, wherein the checksum is usually inserted into the header information for the message (col. 1 lines 53-67) and verified by the receiver comparing the generated checksum with a newly calculated checksum (col. 2 lines 1-16). If the two are equivalent, then no errors are present (col. 2 lines 1-16). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include in the originator/mobile station a checksum component. One of ordinary skill in the art would have been motivated to perform such a modification to detect data transmission errors, as taught by Alferness (col. 1 lines 53-67 & col. 2 lines 1-16).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
June 25, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100